

Domain: <http://demo.testfire.net> & <https://demo.testfire.net> & <http://testphp.vulnweb.com/login.php>

Vulnerability Name	Unencrypted communication (HTTPS Bypassing)
Severity	7.6 - High
CVSS Score	Base Score: 7.6 High CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
Description	Web applications are almost in all cases protected with an SSL/TLS certificate to prevent any MITM attacks and also to maintain the privacy/confidentiality of its users and communication. Typically, TLS certificates will enable the server to communicate with its client in a secure channel which could prevent anyone from interpreting the data in the case of eavesdropping on the network.
Impact & Attack Scenario	While testing the web application we observed that the target application is communicating in an unencrypted channel as a result, an attacker who can monitor the application traffic can see all the requests and responses in plain text.
Vulnerable Location	http://demo.testfire.net https://demo.testfire.net http://testphp.vulnweb.com/login.php
Vulnerable Parameters	HTTP connection
Reproduction Steps	1. Access the following URL: http://testphp.vulnweb.com/login.php 2. <i>Observe that the application is loaded in unencrypted channel (HTTP).</i> & 1. Access the following URL https://demo.testfire.net 2. <i>Intercept the ongoing request to the server, send the request to the repeater.</i> 3. <i>Downgrade the communication from HTTPS to HTTP as shown in the POC image.</i> 4. <i>Send the request to the server and observe 200 OK response code.</i>
Remediation	1. Update the FTP server version to its latest edition. 2. Make sure that security patches are up to date. 3. Disable server version banners in server configuration file. 4. Run FTP service in a low privileged user role. 5. Configure the firewall to block incoming requests to unknown ports/services. 6. Block outgoing requests from an unknown apps.
Sample Code	N/A
Reference	Link1 Link2

Proof of concept:

SendCancel<>

Target: http://demo.testfire.net

Request

PrettyRaw\nActions

1GET / HTTP/1.1
2Host: demo.testfire.net
3Cookie: JSESSIONID=44547F19A38506DC922627CECC7D82E7;
AltoroAccounts=
ODAwMDAwfjNvcnBvcnFOZX4tOS45OTk5NDg2MDUyMTYzOUUxMnw4MDAwMDF+Q2hl
Y2tpbmd+MS4wMDAwMDAxMDkzODIwNDRFMTN8
4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0)
Gecko/20100101 Firefox/120.0
5Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
6Accept-Language: en-US,en;q=0
7Accept-Encoding: gzip, deflat
8Dnt: 1
9Sec-Gpc: 1
10Upgrade-Insecure-Requests: 1
11Sec-Fetch-Dest: document
12Sec-Fetch-Mode: navigate
13Sec-Fetch-Site: none
14Sec-Fetch-User: ?1
15Te: trailers
16Connection: close
17
18

Response

PrettyRawRender\nActions

1HTTP/1.1 200 OK
2Server: Apache-Coyote/1.1
3Set-Cookie: JSESSIONID=C6EC3683DC4B663A64F6E17BC0F6848B; Path=/
4Content-Type: text/html; charset=ISO-8859-1
5Date: Thu, 07 Dec 2023 17:46:56 GMT
6Connection: close
7Content-Length: 9227
8
9
10
11
12
13
14
15
16
17
18
19
20<!-- BEGIN HEADER -->
21<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
22
23<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" >
24
25
26
27<head>

Configure target details

Specify the details of the server to which the request will be sent.
Host: demo.testfire.net
Port: 80
☐ Use HTTPS
OKCancel

0 matches

location:0 matches

Done9,470 bytes | 378 millis

testphp.vulnweb.com/login.php

Connection security for testphp.vulnweb.com

You are not securely connected to this site.
Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).
More information

acunetix

TEST and Demonstration site for Acunetix

homecategoriesartistsdisclaim

search art
go

Browse categories
Browse artists
Your cart
Signup
Your profile

If you are already logged in:
Username :
Password :
login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.